Summary of the thesis entitled

DEVELOPMENT OF FRAMEWORK FOR IMPROVING SECUIRTY MECHANISMS IN DESIGNING DISTRIBUTED SYSTEM

Submitted for partial fulfillment of the award of the Degree of Doctor of Philosophy in Computer Science & Engineering

Vijay Prakash

Robust security and privacy strategies implementation in distributed systems is a challenging issue. This research work makes a step forward in solving this issue by proposing a generic framework for multi-factor authentication to protect services and resources for unauthorized use. The authentication would be based on trust based systems. Proposed framework would not only demonstrate how to obtain secure multi-factor authentication, but also would be addressing several prominent issues bio-inspired computing applications. To deal with different uncertainties in the proposed model fuzzy logic has been used. The rule base systems are implemented using fuzzy knowledge base approach.

1.1 BACKGROUND

A distributed system can be defined as a group of independent computers that appear to the users of the system as a single system, some of the examples of the distributed systems are: network of workstations, automated assembly lines, a network of small office computers. Each computer executes components and works on a distributed middle-ware this distributed middle-ware enables the components to coordinate their activities. The various requirements of distributed systems are categorized into two parts - Application requirements and Non functional requirements.

Application requirements can be functional requirements depending on the centralized system and distributed systems. In non functional requirements various parameter are scalability, concurrency, openness, and resource sharing and fault tolerance. The summarized definitions of these requirements are as follows: Scalability this denotes the ability to accommodate a growing load in the future. Concurrency deals with the execution of different events and conflicting issues. Openness the authorization requirements are totally dependent on the distributed system requirements. Resource sharing offer resources i.e. hardware, software and data required to be shared by more than one user. Distributed objects provide a sophisticated model of Resource sharing. Fault tolerance means that the operation can continue even in the presence of fault and it is achieved in the distributed system by means of replication.

1.2 Cryptography in distributed system security

A cryptosystem is defined as the system which transforms plaintext into cipher text using a key (public or private). The process of designing a cryptosystem is called cryptology whereas the study of cryptosystem is called cryptanalysis. The fusion of cryptology and cryptanalysis is called cryptography. The cryptography is composed of two theories, namely Symmetric key cryptography and Public key cryptography.

This provides security by massage integrity and digital signatures. Several features of the cryptography are as follows.

Confidentiality: In this phase it is ensured that only authenticated sender and intended receiver should understand the original message. In this procedure sender encrypts message and receiver decrypt the message.

End Point Authentication: In this phase the sender and receiver are confirming the identities of each other.

Message Integrity: In this phase the sender and receiver would be ensuring that the original message was not altered during inframsist and after worlds.

Further, to ensure message integrity secured types of approach are used in cryptography such as message digest, internet checksum, Hash Function Algorithm (MDS, SHA-1), Message Authenticate Code (MAC), Digital signature and Public key certificate.

In DNA based cryptography the plain text messages are encoded in the form of DNA which is based are alphabet of short oligonucleotide sequences. The use of DNA improves the compact storage media and an externally small amount of DNA suffices even for a big one time pads.

1.3 PROBLEM STATEMENT

Preserving security and privacy is a challenging issue in distributed systems. This proposal makes a step forward in solving this issue by proposing a generic framework for multi-factor authentication to protect services and resources from unauthorized use. The authentication would be based on trust based model. Proposed framework would not only demonstrate how to obtain secure multi-factor authentication, but also would be addressing several prominent issues of biometric authentication in distributed systems (e.g., client privacy and error tolerance). The model would also be satisfying the Trust Based Model properties.

1.4 MAJOR FINDINGS OF THE PROPOSED WORK

The objectives of the proposed research work are to enhance the security of the distributed system. This proposes the new model of security framework based on the DNA cryptography and computational intelligence approach. The major contributions of the thesis are as follows:

- Computational intelligence approach is used to design a trust based system security framework. Fuzzy logic is used to approximate the trust values of entities in the proposed system.
- DNA cryptography is used to enhance the robustness of designed system. DNA concept is used for the decryption and encryption.